

2) Schumacher's Source Coding Theorem.

We will distinguish the cases of a source emitting pure states $|\varphi_x\rangle$ with probability p_x and that of a source emitting mixed states ρ_x with probability p_x .

2.a) Source of pure states.

Consider a source emitting states $|\varphi_x\rangle$ with probability p_x .

A message is a string of N "letters":

$$|\varphi_{x_1}\rangle \otimes \dots \otimes |\varphi_{x_N}\rangle$$

and has probability $p_{x_1} p_{x_2} \dots p_{x_N}$. If the states $|\varphi_x\rangle$ are mutually orthogonal we are in the same situation than in the classical Shannon Theory. Words are strings $x_1 \dots x_N$ with probabilities $p_{x_1} p_{x_2} \dots p_{x_N}$. The number of "typical words" is

given by $H(p_{x_1}, \dots, p_{x_N}) = N H(X)$. So we expect that

it is possible to faithfully describe this source with NR bits

as long as $R > H(X)$. On the other hand it is not possible to

faithfully describe the source $\square R < H(X)$.

We will see that in the quantum case the same theorem holds with

$H(X)$ replaced by $S(\rho)$. Since in general $S(\rho) < H(X)$

quantum mechanically it is possible to compress more than in the classical

case. This is essentially because the states $\{|\varphi_x\rangle\}$ if not mutually orthogonal are redundant (they cannot be perfectly distinguished).

The method of proof uses as in the classical case the idea of typicality.

Typicality in the classical case.

Let X be a random variable with $\text{Prob}(X=x) = p_x$.

N -strings are said to be ε -typical if they belong to the set

$$A_{N,\varepsilon}(X) = \left\{ (x_1, \dots, x_N) \text{ is a string such that} \right. \\ \left. \left| -\frac{1}{N} \sum_{i=1}^N \log_2 p(x_i) - H(X) \right| < \varepsilon \right\}.$$

The importance of this definition comes from the following

Theorem on typical sequences.

Fix any $\varepsilon > 0$, $\delta > 0$ (small). We can find N sufficiently large such that:

$$(1) \text{Prob}(A_{N,\varepsilon}(X)) \geq 1 - \delta.$$

$$(2) (1-\delta) 2^{N(H(X)-\varepsilon)} \leq |A_{N,\varepsilon}(X)| \leq 2^{N(H(X)+\varepsilon)}$$

(3) Let S_N a collection of strings (x_1, \dots, x_N) with $|S_N| \leq 2^{NR}$ with $R < H(X) - \varepsilon$. Then $\text{Prob}(S_N) \leq \delta$.

Proof. Statement (1) is just the law of large numbers because $H(X) = \mathbb{E}_X (-\log p(x))$ and $-\log p(x_i)$ are i.i.d.

Statement (2) follows from

$$1 - \delta \leq \text{Prob} (A_{N, \epsilon}(X)) \leq 1$$

$$1 - \delta \leq \sum_{x_1, \dots, x_N \in A_{N, \epsilon}(X)} p_{x_1, \dots, x_N} \leq 1 \quad \left. \vphantom{\sum} \right\} \rightarrow (2)$$

and $2^{-N(H(X) - \epsilon)} \leq p_{x_1, \dots, x_N} \leq 2^{-N(H(X) + \epsilon)}$

The third statement follows by splitting $S_N = (S_N \cap A_{N, \epsilon}^c(X)) \cup (S_N \cap A_{N, \epsilon}(X))$.

$$\text{Prob}(S_N \cap A_{N, \epsilon}^c(X)) \leq \delta.$$

$$\begin{aligned} \text{Prob}(S_N \cap A_{N, \epsilon}(X)) &\leq 2^{NR} \cdot 2^{-N(H(X) + \epsilon)} \\ &= 2^{-N(H(X) - R - \epsilon)}. \end{aligned}$$

$\rightarrow 0$ if $R < H(X) - \epsilon$.

Typicality in the quantum case.

In the quantum case we have an analogous Theorem and definition of typicality. Let ρ be a given density matrix.

This has a spectral decomposition

$$\rho = \sum_a \lambda_a |a\rangle\langle a|. \quad \text{or} \quad \sum_a \lambda_a P_a.$$

\uparrow
possibly degenerate.

Here $\lambda_a \geq 0$; $\sum_a \lambda_a = 1$

$P_a = P_a^2$ and $\sum_a P_a = 1$. The Hilbert span is \mathcal{H} .

Consider the Hilbert space $\mathcal{H} \otimes \mathcal{H} \dots \otimes \mathcal{H} = \mathcal{H}^{\otimes N}$.

The projector $P_{N, \epsilon}(\rho)$ onto the "typical subspace" of $\mathcal{H}^{\otimes N}$ is defined as

$$P_{N, \epsilon}(\rho) = \sum_{\substack{a_1, \dots, a_N \\ \text{typical sequences}}} P_{a_1} \otimes P_{a_2} \dots \otimes P_{a_N}$$

where

$$\text{typical sequences} = \left\{ (a_1, \dots, a_N) \mid \left| -\frac{1}{N} \sum_{i=1}^N \log d_{a_i} - S(\rho) \right| < \epsilon \right\}.$$

We have the following theorem (Below $\rho^{\otimes N} = \underbrace{\rho \otimes \rho \otimes \dots \otimes \rho}_{N \text{ times}}$).

Theorem on the typical subspace.

Fix any $\epsilon > 0$, $\delta > 0$ (small). We can find N sufficiently large so that:

$$(1) \quad \text{Tr} (P_{N, \epsilon}(\rho) \cdot \rho^{\otimes N}) \geq 1 - \delta$$

$$(2) \quad (1 - \delta) 2^{N(S(\rho) - \epsilon)} \leq \text{Tr} P_{N, \epsilon}(\rho) \leq 2^{N(S(\rho) + \epsilon)}$$

(3) let S_N be a projector (i.e. $S_N^2 = S_N$) such that $\text{Tr} S_N \leq 2^{NR}$ with $R < S(\rho) - \epsilon$. Then

$$\text{Tr} (S_N \rho^{\otimes N}) \leq \delta.$$

Proof.

Statement 1: Observe that

$$\rho^{\otimes N} = \sum_{a_1, \dots, a_N} \lambda_{a_1} \lambda_{a_2} \dots \lambda_{a_N} \underbrace{P_{a_1} \otimes P_{a_2} \otimes \dots \otimes P_{a_N}}_{\text{mutually orthonormal projectors.}}$$

$$\text{Tr} \left(P_{N, \epsilon}(\rho) \rho^{\otimes N} \right) = \text{Tr} \sum_{\substack{a_1, \dots, a_N \\ \text{typical}}} \lambda_{a_1} \dots \lambda_{a_N} P_{a_1} \otimes P_{a_2} \otimes \dots \otimes P_{a_N}$$

$$= \sum_{\substack{a_1, \dots, a_N \\ \text{typical}}} \lambda_{a_1} \dots \lambda_{a_N}$$

= probability of set of typical sequences where

$$\text{typical sequences} = \left\{ (a_1, \dots, a_N) \mid \left| -\frac{1}{N} \sum_{i=1}^N \log \lambda_{a_i} - S(\rho) \right| < \epsilon \right\}.$$

By the law of large numbers if N sufficiently large:

$$\text{Prob} \left\{ (a_1, \dots, a_N) \mid \left| -\frac{1}{N} \sum_{i=1}^N \log \lambda_{a_i} - \underbrace{\sum_a \lambda_a (-\log \lambda_a)}_{S(\rho)} \right| < \epsilon \right\} \geq 1 - \delta.$$

Therefore $\text{Tr} \left(P_{N, \epsilon}(\rho) \rho^{\otimes N} \right) \geq 1 - \delta.$

Statement 2: Observe that $\text{Tr} P_{N, \epsilon}(\rho) = \sum_{\substack{a_1, \dots, a_N \\ \text{typical}}} 1 = \# \text{ (of typ sequences)}.$

So the argument is the same than in the classical case.

Statement 3:

Observe that:

$$\text{Tr } S_N \rho^{\otimes N} = \text{Tr} (S_N \rho^{\otimes N} P_{N,\varepsilon}(\rho)) + \text{Tr} S_N \rho^{\otimes N} (\mathbb{I} - P_{N,\varepsilon}(\rho))$$

$$\begin{aligned} * \text{Tr } S_N \rho^{\otimes N} P_{N,\varepsilon}(\rho) &= \text{Tr } S_N \rho^{\otimes N} P_{N,\varepsilon}(\rho) S_N \quad (\text{cyclic}) \\ &= \text{Tr } S_N P_{N,\varepsilon}(\rho) \rho^{\otimes N} P_{N,\varepsilon}(\rho) S_N \\ &\quad (P_{N,\varepsilon}(\rho) \text{ and } \rho^{\otimes N} \text{ commute}). \end{aligned}$$

$$\leq \frac{-N(S(\rho) - \varepsilon)}{2} \text{Tr } S_N$$

$$\leq \frac{-N(S(\rho) - R - \varepsilon)}{2} \rightarrow 0 \text{ if } R < S(\rho) - \varepsilon.$$

$$* \text{Tr } S_N \rho^{\otimes N} (\mathbb{I} - P_{N,\varepsilon}(\rho)) = \text{Tr } S_N \underbrace{\rho^{\otimes N} (\mathbb{I} - P_{N,\varepsilon}(\rho))}_{(\mathbb{I} - P_{N,\varepsilon}(\rho))}$$

and $\underbrace{(\mathbb{I} - P_{N,\varepsilon}(\rho)) \rho^{\otimes N} (\mathbb{I} - P_{N,\varepsilon}(\rho))}_M$ is positive so by cyclicity

$$\text{Tr } S_N \rho^{\otimes N} (\mathbb{I} - P_{N,\varepsilon}(\rho)) = \text{Tr } M^{1/2} S_N M^{1/2}$$

$$\leq \text{Tr } M^{1/2} \mathbb{I} M^{1/2}$$

$$\leq \text{Tr } M = \text{Tr } \rho^{\otimes N} (\mathbb{I} - P_{N,\varepsilon}(\rho))$$

$$\leq \delta.$$

Encoding - Decoding operations.

* Suppose that the input word is $|\varphi_{x_1}\rangle \otimes \dots \otimes |\varphi_{x_N}\rangle$.
 (this has a probability $p_{x_1} \dots p_{x_N}$). We expect the encoding operation to compress this word to a string of M qubits so an element of the Hilbert space $\mathbb{C}_2^{\otimes M} = \underbrace{\mathbb{C}_2 \otimes \dots \otimes \mathbb{C}_2}_{M \text{ times}}$.

We allow for a slightly more general definition of the encoding map:

$$\mathcal{E} : \mathcal{H}^{\otimes N} \rightarrow \left\{ \text{Density matrices of } \mathbb{C}_2^{\otimes M} \right\}$$

$$|\varphi_{x_1}\rangle \otimes \dots \otimes |\varphi_{x_N}\rangle \mapsto \rho_M(x_1, \dots, x_N).$$

where ρ_M is a $2^M \times 2^M$ density matrix. We require $M < N$ which corresponds to compression. The rate of the encoder is

$$R = \frac{M}{N} < 1.$$

* The decoding operation is a map:

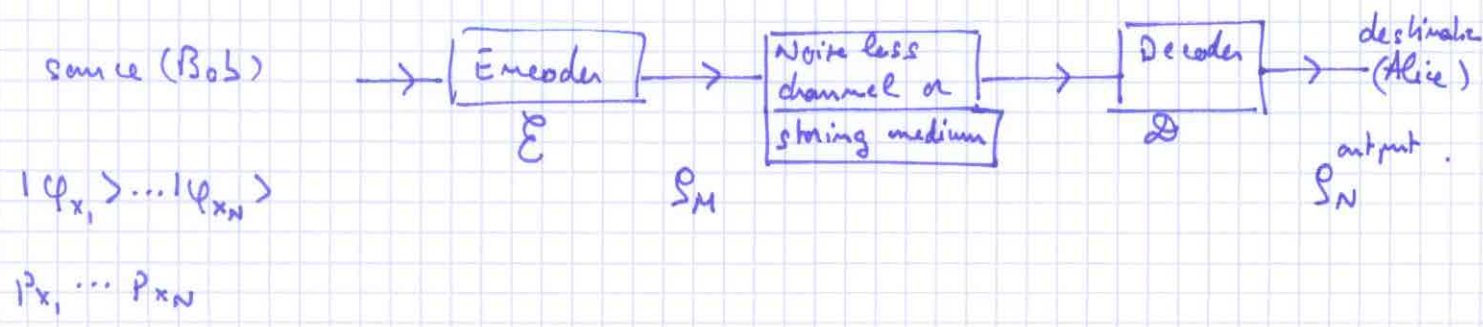
$$\mathcal{D} : \left\{ \text{Density matrices of } \mathbb{C}_2^{\otimes M} \right\} \rightarrow \left\{ \text{Density matrices of } \mathcal{H}^{\otimes N} \right\}$$

$$\rho_M(x_1, \dots, x_N) \mapsto \overset{\text{output}}{\rho_N}(x_1, \dots, x_N).$$

Ideally we would like to recover the input word so we would like to have

$$\overset{\text{output}}{\rho_N}(x_1, \dots, x_N) = (|\varphi_{x_1}\rangle \otimes \dots \otimes |\varphi_{x_N}\rangle) (\langle \varphi_{x_1}| \otimes \dots \otimes \langle \varphi_{x_N}|)$$

The block diagram of the encoding-decoding scheme is



Reliability criterion.

Given that $|\psi_{x_1}, \dots, \psi_{x_N}\rangle$ was sent we define the "Fidelity" as

$$F(x_1, \dots, x_N) = \langle \psi_{x_1}, \dots, \psi_{x_N} | S_N^{\text{output}} | \psi_{x_1}, \dots, \psi_{x_N} \rangle.$$

The motivation for this definition is that if the transmittion is ideal we have $F = 1$. Moreover if the letters $\{|\psi_x\rangle\}$ are all mutually orthogonal and $S_N^{\text{output}} = |\psi_{y_1}, \dots, \psi_{y_N}\rangle \langle \psi_{y_1}, \dots, \psi_{y_N}|$ then we are reduced to the classical case where

$$F(x_1, \dots, x_N) = \begin{cases} 1 & \text{if } (x_1, \dots, x_N) = (y_1, \dots, y_N) \\ 0 & \text{if not} \end{cases}$$

The average Fidelity is

$$F = \sum_{x_1, \dots, x_N} p_{x_1} \dots p_{x_N} \langle \psi_{x_1}, \dots, \psi_{x_N} | S_N^{\text{output}} | \psi_{x_1}, \dots, \psi_{x_N} \rangle.$$

In the classical case this reduces to the probability of Block error. Hereafter we take the average fidelity as our notion of reliability. Note that one can make other definitions and it is not a priori

obvious that they are all equivalent. We are now ready to formulate our main theorem:

Theorem [Quantum Source Coding - Schumacher 1995]

Consider a source prepared with the ensemble $\{p_x, |\varphi_x\rangle\}$.

Take any $\epsilon > 0$, $\delta > 0$ (small).

(A) Achievability part: Let $R > S(\rho) + \epsilon$. There exist an encoding-decoding scheme $(\mathcal{E}, \mathcal{D})$ with rate R such that for N sufficiently large $F \geq 1 - \delta$.

(B) Converse part: Let $R < S(\rho) - \epsilon$. For any scheme $(\mathcal{E}, \mathcal{D})$ with rate R we have for N sufficiently large that $F \leq \delta$.

Proof of Achievability:

As in the classical Shannon theorem the main idea is to encode and decode faithfully ^{only} the words that belong to the typical subspace. This will basically require $N S(\rho)$ qubits. The rest of the words have small probability of occurrence so the probability of error will be small. The details are as follows:

Encoding operation:

Given an input word $|\varphi_{x_1}, \dots, \varphi_{x_N}\rangle$ do a measurement in

the basis $(P_{N, \epsilon}(\rho); I - P_{N, \epsilon}(\rho))$. The outcome is

$$\frac{P_{N,\epsilon}(\rho) |\varphi_{x_1} \dots \varphi_{x_N}\rangle}{\langle \varphi_{x_1} \dots \varphi_{x_N} | P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N} \rangle}^{1/2}$$

$$\text{with prob} = \langle \varphi_{x_1} \dots \varphi_{x_N} | P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N} \rangle$$

or

$$\frac{(I - P_{N,\epsilon}(\rho)) |\varphi_{x_1} \dots \varphi_{x_N}\rangle}{\langle \varphi_{x_1} \dots \varphi_{x_N} | I - P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N} \rangle}^{1/2}$$

$$\text{with prob} = \langle \varphi_{x_1} \dots \varphi_{x_N} | I - P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N} \rangle$$

* If the outcome belongs to the typical subspace (first case) then the state $P_{N,\epsilon}(\rho) |\varphi_{x_1} \dots \varphi_{x_N}\rangle$ has at most $2^{N(S(\rho)+\epsilon)}$ non zero components. Note that the typical subspace vectors all have at most $2^{N(S(\rho)+\epsilon)}$ non zero components. This means that by a transposition (or permutation) of components we can package all these vectors in a $2^{N(S(\rho)+\epsilon)}$ dim vector (with the rest of the components being zero). This operation can be represented by a unitary matrix U ;

$$U P_{N,\epsilon}(\rho) |\varphi_{x_1} \dots \varphi_{x_N}\rangle = \sum_{\substack{b_1 \dots b_M \\ c_{x_1} \dots c_{x_N}}} | \underbrace{b_1 \dots b_M}_{\mathbb{C}_2^{\otimes M}} , \underbrace{0, 0 \dots 0}_{N-M} \rangle$$

$$= | \psi_{x_1 \dots x_N}^{\text{compressed}} \rangle \otimes | \underbrace{0, 0 \dots 0}_{N-M} \rangle$$

One sends $| \psi_{x_1 \dots x_N}^{\text{compressed}} \rangle$ which is a M -qubit state.

* If the outcome belongs to the α -typical subspace

(second case) the state $(I - P_{N\epsilon}(\rho)) |\varphi_{x_1} \dots \varphi_{x_N}\rangle$ is coded as a "junk state". In other words we send just $|junk\rangle$

which is a specified state of the typical subspace, say

Thus at the output of the encoder,

the density matrix is

$$\sigma = \langle \varphi_{x_1} \dots \varphi_{x_N} | P_{N\epsilon} | \varphi_{x_1} \dots \varphi_{x_N} \rangle \cdot | \overset{\text{compressed}}{\varphi_{x_1 \dots x_N}} \rangle \langle \overset{\text{compressed}}{\varphi_{x_1 \dots x_N}} | + \langle \varphi_{x_1} \dots \varphi_{x_N} | I - P_{N\epsilon} | \varphi_{x_1} \dots \varphi_{x_N} \rangle \cdot | junk \rangle \langle junk |$$

To summarize the encoder maps

$$\mathcal{E}: |\varphi_{x_1} \dots \varphi_{x_N}\rangle \langle \varphi_{x_1} \dots \varphi_{x_N}| \rightarrow \sigma$$

Decoding Operation.

The input to the decoder is σ . First one appends the $(N-M)$ 0 states that were discarded before. Then one applies the inverse transposition or permutation (a unitary operation) to recover

$$P_{N,\epsilon} |\varphi_{x_1} \dots \varphi_{x_N}\rangle$$

$$\langle \varphi_{x_1} \dots \varphi_{x_N} | P_{N,\epsilon} | \varphi_{x_1} \dots \varphi_{x_N} \rangle^{1/2}$$

So the decoder maps: $\mathcal{D} : \sigma \rightarrow \rho^{\text{output}}$ with

$$\rho^{\text{output}} = P_{N,\epsilon} |\varphi_{x_1} \dots \varphi_{x_N}\rangle \langle \varphi_{x_1} \dots \varphi_{x_N}| P_{N,\epsilon} \\ + \langle \varphi_{x_1} \dots \varphi_{x_N} | (\mathbb{I} - P_{N,\epsilon}) | \varphi_{x_1} \dots \varphi_{x_N}\rangle U | \text{junk}, 0_{N-M}\rangle \langle \text{junk}, 0_{N-M}| U^\dagger$$

It remains to estimate the Fidelity of this scheme.

$$F = \sum_{x_1, \dots, x_N} p_{x_1} \dots p_{x_N} \langle \varphi_{x_1} \dots \varphi_{x_N} | \rho^{\text{output}} | \varphi_{x_1} \dots \varphi_{x_N}\rangle.$$

* The first contribution is

$$\sum_{x_1, \dots, x_N} p_{x_1} \dots p_{x_N} \left| \langle \varphi_{x_1} \dots \varphi_{x_N} | P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N}\rangle \right|^2$$

$$\geq \left\{ \sum_{x_1, \dots, x_N} p_{x_1} \dots p_{x_N} \langle \varphi_{x_1} \dots \varphi_{x_N} | P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N}\rangle \right\}^2 \quad (\text{Schwarz inequality})$$

$$= \left\{ \text{Tr}(\rho^{\otimes N} P_{N,\epsilon}(\rho)) \right\}^2 \geq (1-\delta)^2 \quad (\text{by theorem on typical subspace}).$$

* The second contribution is

$$\sum_{x_1, \dots, x_N} p_{x_1} \dots p_{x_N} \langle \varphi_{x_1} \dots \varphi_{x_N} | \mathbb{I} - P_{N,\epsilon}(\rho) | \varphi_{x_1} \dots \varphi_{x_N}\rangle \\ \cdot \left| \langle \varphi_{x_1} \dots \varphi_{x_N} | U | \text{junk}, 0_{N-M}\rangle \right|^2 \geq 0.$$

This proves the achievability part.

Proof of the converse.

Let $\mathcal{E} : |\varphi_{x_1} \dots \varphi_{x_N}\rangle \langle \varphi_{x_1} \dots \varphi_{x_N}| \rightarrow \sigma$ be a general encoding scheme. Before decoding we append $|0_{N-M}\rangle \langle 0_{N-M}|$ as before so the input to the decoder is

$$\sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}|.$$

This state belongs to a $2^M = 2^{NR}$ subspace of $\mathcal{H}^{\otimes N}$ with $R < S(\rho) - \epsilon$. Let S_N be the projector on this subspace. We have

$$S_N \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| S_N = \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}|.$$

Now we restrict ourselves to a unitary decoder \mathcal{D} as before:

$$\mathcal{D} : \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| \rightarrow U \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| U^\dagger.$$

$$\begin{aligned} \text{So } \rho^{\text{output}} &= U \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| U^\dagger \\ &= U S_N \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| S_N U^\dagger. \end{aligned}$$

The fidelity is

$$\begin{aligned} F &= \sum_{x_1, \dots, x_N} p_{x_1} \dots p_{x_N} \langle \varphi_{x_1} \dots \varphi_{x_N} | U S_N \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| S_N U^\dagger | \varphi_{x_1} \dots \varphi_{x_N} \rangle \\ &= \text{Tr} \left(\rho^{\otimes N} U S_N \sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| S_N U^\dagger \right) \\ &= \text{Tr} \left(S_N U^\dagger \rho^{\otimes N} U S_N \right) \left(\sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}| \right). \end{aligned}$$

Since $S_N U^\dagger \rho^{\otimes N} U S_N$ is a positive operator and

$\sigma \otimes |0_{N-M}\rangle \langle 0_{N-M}|$ is a density matrix and then ≤ 1

we obtain

$$F \leq \text{Tr} S_N U^\dagger \rho^{\otimes N} U$$

$$= \text{Tr} (U S_N U^\dagger) \rho^{\otimes N}.$$

Now $U S_N U^\dagger$ is a projector on a 2^{NR} subspace with $R < S(\rho) - \epsilon$.
 Then by the third statement of the typical subspace theorem we have $\bar{F} \leq \delta$.

This achieves the proof of the converse for unitary decodings.
 For non-unitary decodings the proof is more difficult and is omitted here. \blacksquare

2.6) Source of mixed states.

For a source emitting mixed states ρ_x with probabilities p_x , the input messages are strings of N "letters"

$$\rho_{x_1} \otimes \dots \otimes \rho_{x_N}.$$

In this case it is known that a rate $R < \chi(\rho) = S(\rho) - \sum p_x S(\rho_x)$ is not achievable (whatever the encoding-decoding scheme). However it is not known if a rate $R > \chi(\rho)$ is achievable although this is conjectured to be the case.

The proof that $R < \chi(\rho)$ is not achievable will be omitted in these notes.